لآ اِلَهَ اِلّا اللّهُ مُحَمَّدٌ رَسُوُل اللّهِ

মুজাহিদের অনলাইন সিকিউরিটি

313C7R0_544D

How to Stay Anonymous

By 313C7R0_544D

অনুবাদ

Green Bird Media

আমাদের ফোরামে আপনাকে স্বাগতম – www.dawahilallah.com

নির্যাতিত উম্মাহ এবং সারা বিশ্বের মুজাহিদীনের খবরাখবর পেতে ভিজিট করুন – www.gazwah.net

মুজাহিদ শায়েখ এবং উমারাগণের লেখনী সমূহ পেতে ভিজিট করুন – www.darulilm.org

বিসমিল্লাহির রাহমানির রাহীম

অনলাইনে পরিচয় গোপন রাখার উপায়

একজন অ্যানোনিমাস হ্যাকারের (**313C7R0_544D**) পক্ষ থেকে

আসসালামু আলাইকুম,

এই বইটি সারা বিশ্বে জিহাদ-ফি-সাবিলিল্লাহ তে অংশগ্রহণকারী সকল মুজাহিদীনের জন্য।

আমাদের মত হ্যাকারদের কর্তৃপক্ষ থেকে নিরাপদে থাকার জন্য এসকল অনলাইন সিকিউরিটি অবলম্বন করা অত্যাবশ্যক। জিহাদের ময়দানে আমাদের অনেক ভাই আছেন যারা এ ব্যাপারে খুব বেশি ধারণা রাখেন না, তাই আমি সিদ্ধান্ত নিয়েছি কিভাবে সরকারি গোয়েন্দা বাহিনীর হাত থেকে নিরাপদে থাকা যায় সে ব্যাপারে একটি আর্টিকেল লিখার।

যদি আপনি মনোযোগ দিয়ে এটি পড়েন তাহলে ইনশাআল্লাহ আপনার অনলাইন আইডেন্টিটি গোপন রাখার ব্যাপারে অনেক কিছু শিখতে পারবেন।

আর্টিকেলটি কিছুটা বড় হবে যেন বিভিন্ন বিষয় সাধারণ ভাইদের বুঝার সুবিধার্থে ব্যাখ্যা করা যায়, কাজেই আলসেমি করে কোনো কিছু বাদ দিয়ে যাবেন না , প্রথম থেকে শেষ পর্যন্ত ধৈর্য্য সহকারে পড়ুন। এই সামান্য ১৫/২০ মিনিট আপনাকে ৫/১০/১৫ বছর কারাগারে থাকা থেকে বাঁচাতে পারে। আমি আমার প্রভু আল্লাহ আজ্জা-ওয়া-জাল এর কাছ থেকেই এ কাজের প্রতিদান আশা করি। কাজটিকে সহজভাবে করার জন্য আমি অন্যান্য আর্টিকেল থেকে সাহায্য নিব।

হ্যাকিং এর জন্য অত্যন্ত গুরুত্বপূর্ণ বিষয় হল পরিচয় গোপন রাখা। নিজের পরিচয় গোপন না রেখে কোনো কিছু হ্যাক করা আসলে অর্থহীন। উদাহরণ স্বরূপ, মনে করুন আপনি কারো ওয়াইফাই হ্যাক করেছেন কিংবা আপনি অনলাইনে জিহাদ-ফি-সাবিলিল্লাহ সম্পর্কিত কাজ করছেন কিন্তু আপনার পরিচয় গোপন করেন নি। কিছুদিন পর পুলিশ ঐ ওয়াইফাই রাউটার অ্যানালাইসিস করবে এবং সেখানে আপনার কম্পিউটারের ইনফরমেশন খুঁজে পাবে। অবশেষে তারা আপনাকে ধরে ফেলবে এবং কারাগারে নিক্ষেপ করবে। কাজেই হ্যাকিং কিংবা অনলাইনে অজ্ঞাতপরিচয়(অ্যানোনিমাস) থাকার ক্ষেত্রে অত্যন্ত গুরুত্বপূর্ণ বিষয় হচ্ছে নিজের পরিচয় গোপন রাখা এবং হ্যাকিংকে আন্ট্রেসেবল বানানো। এখানে আমরা শিখবো কিভাবে অ্যানোনিমাস হওয়া যায়, পরিচয় গোপন রাখতে হয় এবং সম্পূর্ণরূপে আনট্রেসেবল হওয়া যায়।

 # ম্যাক এড্রেস কি?

একটি ম্যাক (MAC-Media Access Control) এড্রেস হল ফিজিক্যাল নেটওয়ার্ক সেগমেন্টে যোগাযোগের জন্য নেটওয়ার্কিং যন্ত্রগুলোতে বরাদ্দকৃত অনন্য একটি এড্রেস। প্রতিটি কম্পিউটার

ডিভাইসের আলাদা আলাদা ম্যাক এড্রেস রয়েছে। কম্পিউটারগুলো তৈরি করার সময় এদেরর জন্য ভিন্ন ভিন্ন ম্যাক এড্রেস বরাদ্দ হয়ে যায়। যখন কম্পিউটার চালু হয় তখন অপারেটিং সিস্টেম হার্ডওয়্যারের তথ্যগুলো সংগ্রহ করে। যখন আপনি ওয়্যারলেস নেটওয়ার্কে কানেক্ট হন এটা আপনাকে প্যাকেট পাঠায় এবং আপনার কম্পিউটার এই প্যাকেটগুলোকে ওয়েবসাইট, মুভি কিংবা ইমেজে কনভার্ট করে। এখন মনে করুন ওয়ারলেস নেটওয়ার্কে দুটি কম্পিউটার সংযুক্ত আছে, প্রথম কম্পিউটারটি google.com এ যেতে চায় এবং দ্বিতীয়টি amazon.com এ যেতে চায়। নেটওয়ার্ক দুটি কম্পিউটারেই প্যাকেট পাঠায়। এখন কম্পিউটার দুটি কিভাবে বুঝবে কোন প্যাকেট গ্রহণ করতে হবে আর কোনটা ইগনোর করতে হবে? এক্ষেত্রে কম্পিউটার ম্যাক এড্রেস ব্যবহার করে প্যাকেট আইডেন্টিফাই করে। যখন নেটওয়ার্ক প্যাকেট পাঠায় তখন যে কম্পিউটারের জন্য সেটা পাঠায় সে কম্পিউটারের ম্যাক এড্রেস প্যাকেটের সাথে সংযুক্ত করে দেয়। এভাবেই ওয়ারলেস নেটওয়ার্ক এবং কম্পিউটারের মধ্যে সংযোগ সাধিত হয়। কাজেই যদি আপনি আপনার ম্যাক এড্রেস পরিবর্তন না করে কারো ওয়ারলেস নেটওয়ার্ক হ্যাক করেন, তার মানে আপনি তাকে নেটওয়ার্ক হিস্টোরি অ্যানালাইজ করে আপনার পরিচয় খুঁজে পাওয়ার ব্যবস্থা করে দিচ্ছেন।

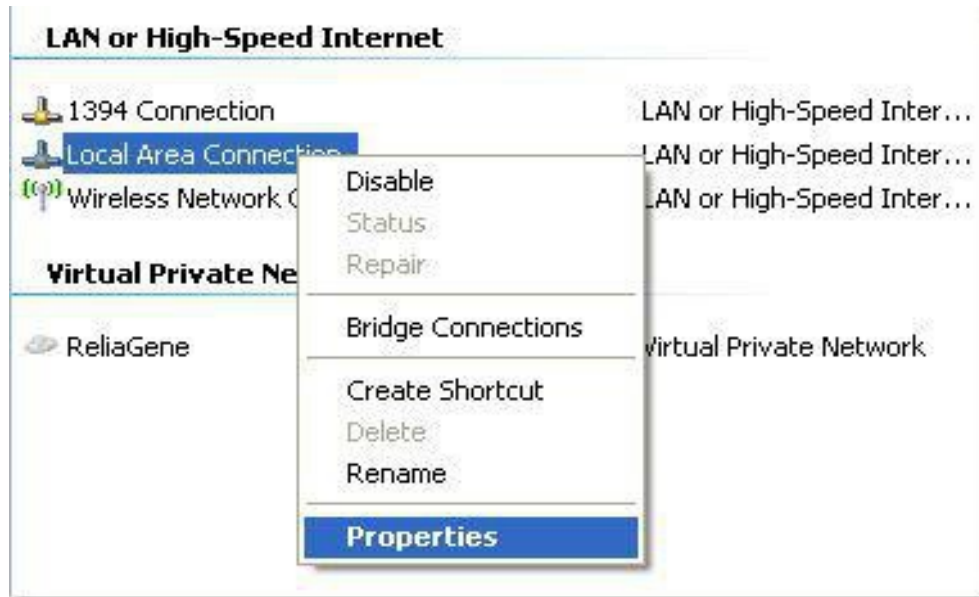
 # কিভাবে ম্যাক এড্রেস পরিবর্তন করবেন?

আপনার মনে হয়তো প্রশ্ন জাগতে পারে, কিভাবে ম্যাক এড্রেস পরিবর্তন করা সম্ভব যেখানে কম্পিউটার এটা হার্ডওয়্যার থেকে সংগ্রহ করে থাকে? আসলে আপনাকে এর জন্য হার্ডওয়্যারে মডিফিকেশন করতে হবে না বরং আপনাকে র‍্যামের তথ্য পরিবর্তন করলেই হবে। কম্পিটার চালু হওয়ার সময় ম্যাক এড্রেস কম্পিউটারের র‍্যামে সংরক্ষিত হয় , আমরা র‍্যামে থাকা এই ম্যাক এড্রেস পরিবর্তন করব..।

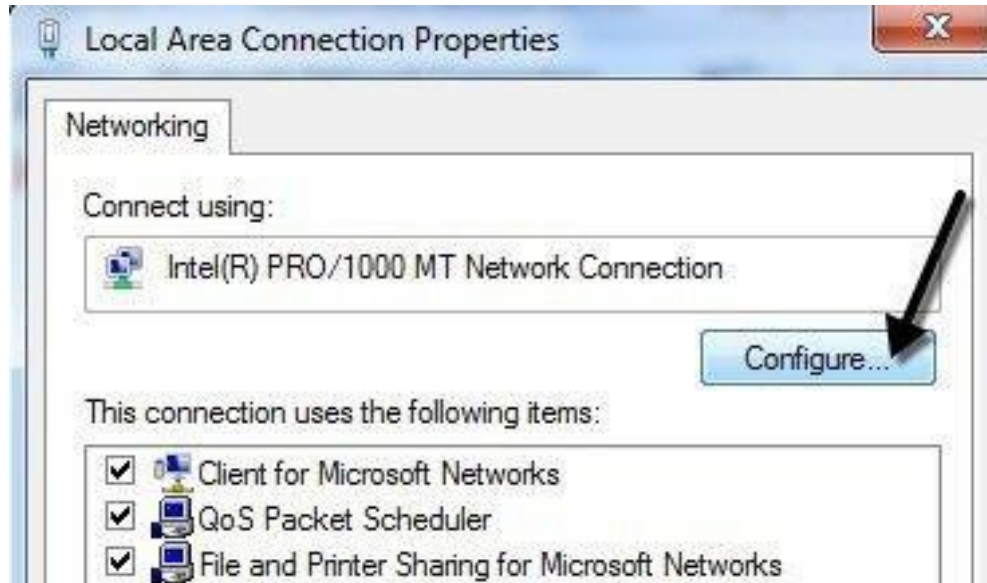
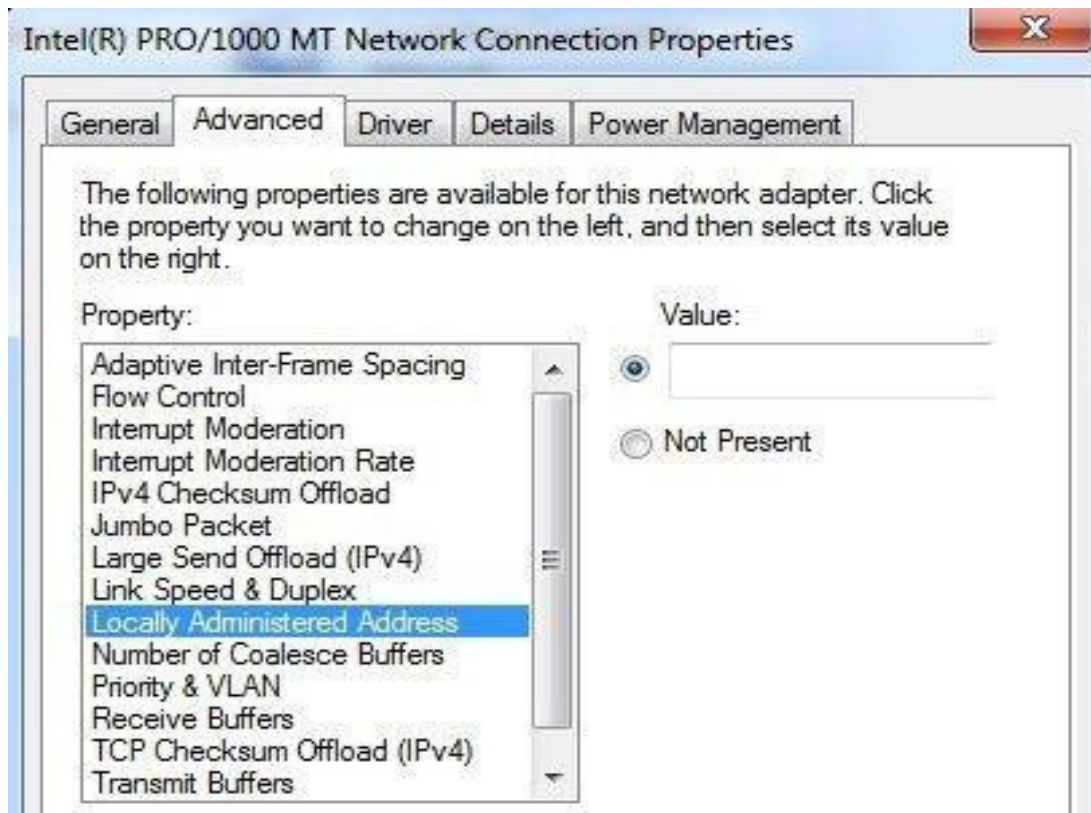
এভাবে যখন আপনি আপনার ম্যাক এড্রেস পরিবর্তন করবেন তখন পুলিশ আপনার ফেক ম্যাক এড্রেস খুঁজে পাবে এবং তারা আপনাকে ধরতে সক্ষম হবে না। আশা করি আপনি এখন ম্যাক এড্রেস কি, ম্যাক এড্রেস পরিবর্তন না করে হ্যাকিং কিংবা অনলাইনে জিহাদী কাজ করার বিপদ, পুলিশ কিভাবে আপনাকে খুঁজে পেতে পারে এবং কিভাবে আমরা ম্যাক এড্রেস পরিবর্তন করতে পারি এ ব্যাপারে ব্যাসিক ধারনা পেয়েছেন।

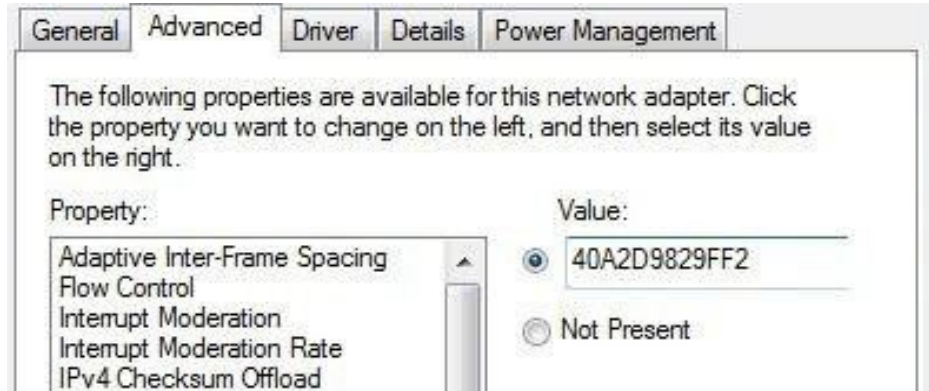
Windows এর ম্যাক এড্রেস পরিবর্তন:

নিচের ধাপগুলো অনুসরণ করে আপনি খুব সহজেই Windows এর নেটওয়ার্ক কার্ডের MAC Address পরিবর্তন করতে পারবেন।

ধাপ ১: Start এ ক্লিক করুন, এরপর Control Panel এ গিয়ে Network Connections এ যান এবং যে নেটওয়ার্ক কানেকশনের ম্যাক এড্রেস পরিবর্তন করতে চান (এটা সাধারণত Local Area Connection অথবা Wireless Network Connection নামে থাকে) তাতে মাউস পয়েন্টার রেখে রাইট বাটনে ক্লিক করুন এবং Properties সিলেক্ট করুন।

যদি আপনি Windows Vista, Windows 7 কিংবা উচ্চতর কোনো ভার্সন ব্যাবহার করেন তাহলে আপনাকে Control Panel এ গিয়ে সেখান থেকে Network and Sharing Center এ গিয়ে Manage Network Connections কিংবা Change adapter settings এ ক্লিক করতে হবে।

সেখান থেকে Adapter এ রাইট-ক্লিক করে Properties এ যেতে হবে।

ধাপ ২: General কিংবা Networking ট্যাব এ Configure বাটনে ক্লিক করুন।

ধাপ ৩: এখন Advanced Tab এ ক্লিক করুন এরপর Locally Administered Address property কিংবা Network Address property তে ক্লিক করুন।

এখানে Not Present রেডিও বাটন সিলেক্ট করা থাকবে , আপনাকে Value রেডিও বাটনটি সিলেক্ট করতে হবে এবং পাশের বক্সে একটি নতুন ম্যাক এড্রেস লিখে দিতে হবে। ম্যাক এড্রেস হল ৬ জোড়া নাম্বার এবং ক্যারেক্টারের সমন্বয়ে তৈরি একটি এড্রেস, যেমন- A2-D9-82-9F-F2 ।

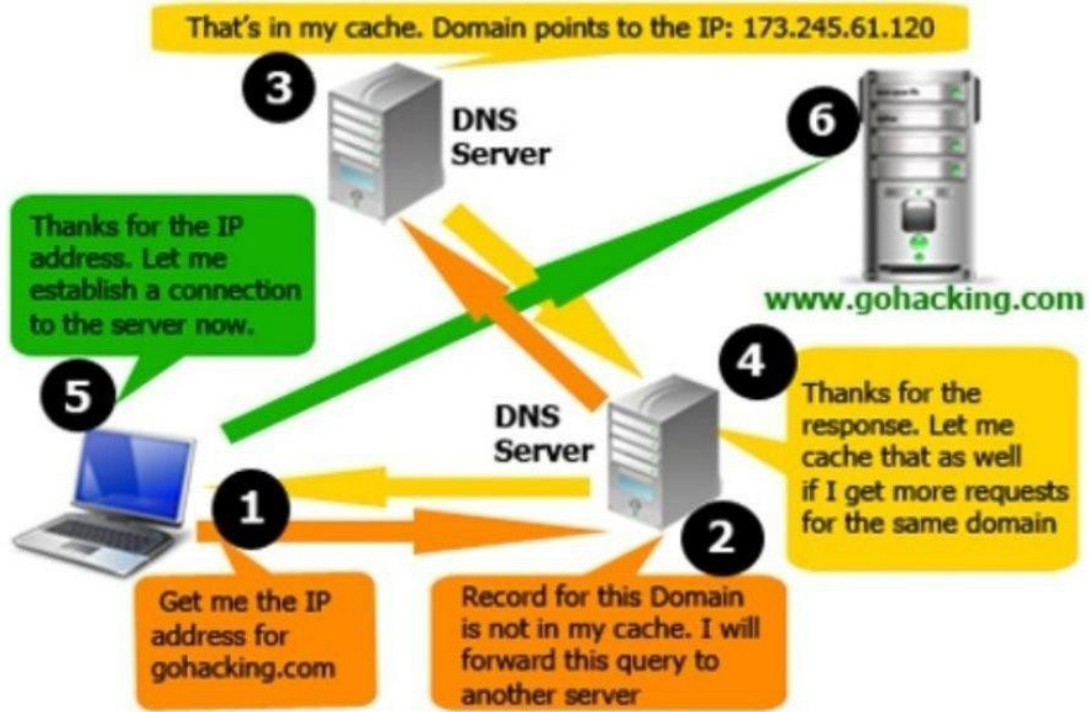
এড্রেসটি লিখার সময় ড্যাশ বাদ দিয়ে লিখতে হবে।

ম্যাক এড্রেস পরিবর্তিত হয়েছে কিনা তা চেক করতে Command Prompt এ গিয়ে IPCONFIG/ALL টাইপ করে Enter চাপুন। (Start Menu তে গিয়ে cmd লিখে সার্চ করলেই cmd.exe পেয়ে যাবেন। এটাই Command Prompt) । এখন কম্পিউটার রিস্টার্ট দিন যেন পরিবর্তিত ম্যাক এড্রেসটি কার্যকর হয়।

উপরে বর্ণিত পদ্ধতি আপনার জন্য কাজ না করলে দুঃখিত হবেন না। আপনি যেহেতু ম্যাক এড্রেস সম্পর্কে অনেক কিছু জেনেছেন কাজেই আপনি নিজেই এখন আপনার কম্পিউটারের জন্য উপযুক্ত পদ্ধতি খুঁজে বের করতে পারবেন। Youtube এ আপনার অপারেটিং সিস্টেম (যেমন- Windows 7, Windows 8.1, Windows 10, Linux ইত্যাদি) লিখে সার্চ দিন কিভাবে এর ম্যাক এড্রেস পরিবর্তন করা যায়। ইনশাআল্লাহ পেয়ে যাবেন।

আলহামদুলিল্লাহ। একসাথে এত বেশি চাপ নেয়ার প্রয়োজন নেই। পরবর্তী অংশে যাওয়ার আগে একটি চা বিরতি নিয়ে আপনার ব্রেইনকে ফ্রেশ করে নিন।

#DNS এড্রেস কী?

DNS সার্ভার হল এমন একটি কম্পিউটার সার্ভার যেখানে বিভিন্ন পাবলিক আইপি এড্রেস এবং তাদের হোস্টনেম এর ডাটাবেস সংরক্ষিত থাকে। এই সার্ভার সাধারণত ব্যবহারকারীর চাওয়া এসব হোস্টনেমকে (www.google.com, www.kalamullah.com ইত্যাদি) তাদের আইপি এড্রেসে ট্রান্সলেট করে।

DNS সার্ভারগুলোতে বিশেষ কিছু সফটওয়্যার থাকে এবং এরা বিশেষ প্রটোকল ব্যবহার করে নিজেদের মধ্যে যোগাযোগ রক্ষা করে।

আরো সহজ ভাষায় বলতে গেলে – DNS সার্ভার হল ইন্টারনেটে থাকা একটি ডিভাইস, আপনি যখন আপনার ব্রাউজারে www.lifewire.com টাইপ করেন তখন এই ডিভাইসটি বলে দেয় যে সেটার আইপি এড্রেস হল 151.101.129.121 যা ওয়েবসাইটটির আসল ঠিকানা।

DNS সার্ভার থাকতে হবে কেন??

অন্য একটি প্রশ্নের মাধ্যমে এই প্রশ্নের জবাব দেয়া যায়— বলুনতো 151.101.129.121 মনে রাখা সহজ নাকি www.lifewire.com?? নিঃসন্দেহে একটি লম্বা নাম্বার স্ট্রিং মনে রাখার চেয়ে lifewire এর মত একটি শব্দ মনে রাখা সবার জন্য সহজ।

যখন আপনি ওয়েব ব্রাউজারে www.lifewire.com এ যান, আপনাকে শুধু এইটুকু বুঝলে এবং মনে রাখলেই হয় যে URL টি হল https://www.lifewire.com । অন্যান্য ওয়েবসাইট যেমন google.com, amazon.com এর ক্ষেত্রেও এমন।

অপরদিকে, আমরা মানুষ হিসেবে যেমন URL এ থাকা শব্দগুলো আইপি এড্রেস নাম্বারের চেয়ে সহজে বুঝতে পারি তেমন কম্পিউটার কিংবা নেটওয়ার্ক ডিভাইসগুলো আইপি এড্রেস সহজে বুঝতে পারে।

তাই আমাদের DNS সার্ভার প্রয়োজন কেননা ওয়েবসাইট এক্সেস করার জন্য শুধু আমাদের এর পাঠযোগ্য নাম ব্যবহার করতে চাইলেই চলবে না বরং কম্পিউটার ওয়েবসাইট এক্সেস করার জন্য আইপি এড্রেস চাইবে। DNS সার্ভারই হল হোস্টনেম এবং আইপি এড্রেসের মধ্যকার এই ট্রান্সলেটর।

কিভাবে DNS সার্ভার পরিবর্তন করবেন??

আমরা আমাদের DNS এড্রেস Cloudfare এ পরিবর্তন করব কেননা এটা সবচেয়ে নিরাপদ এবং খুবই দ্রুতগতিসম্পন্ন সার্ভার।

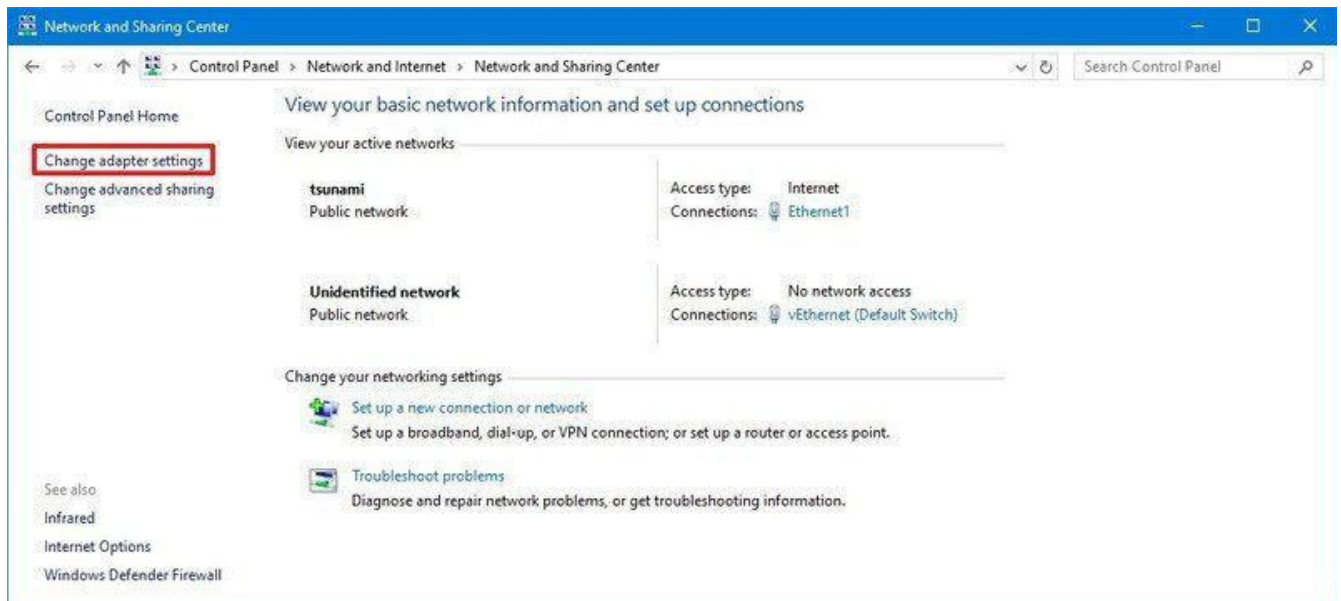
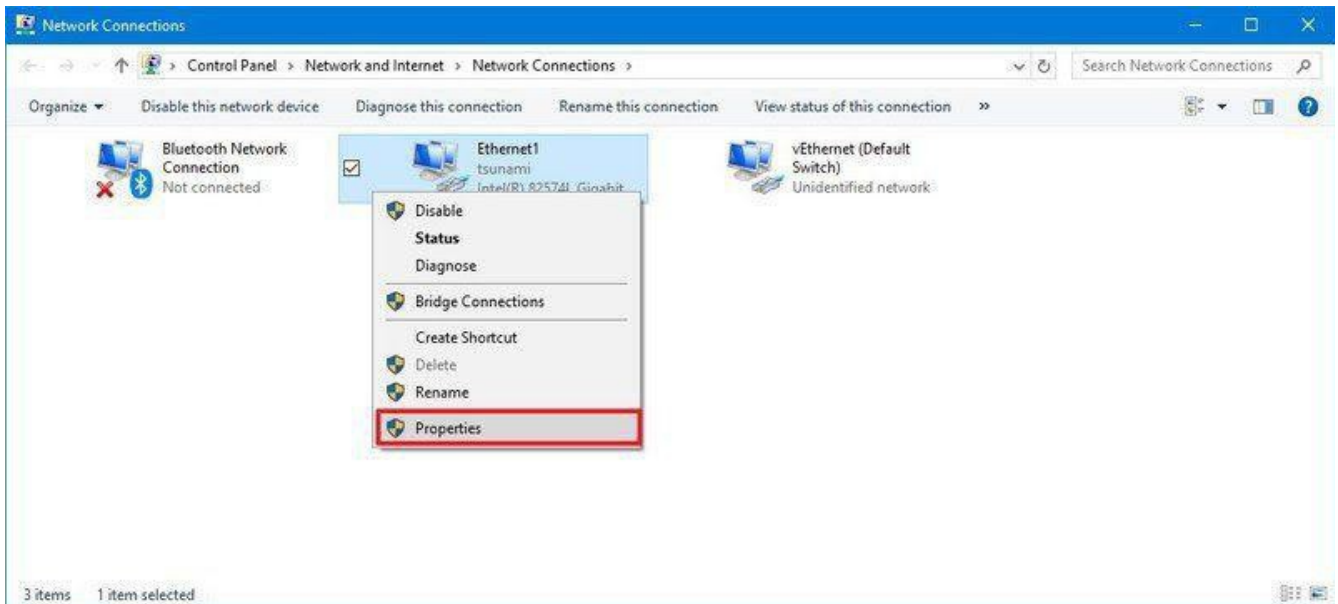
DNS Address পরিবর্তনের জন্য –

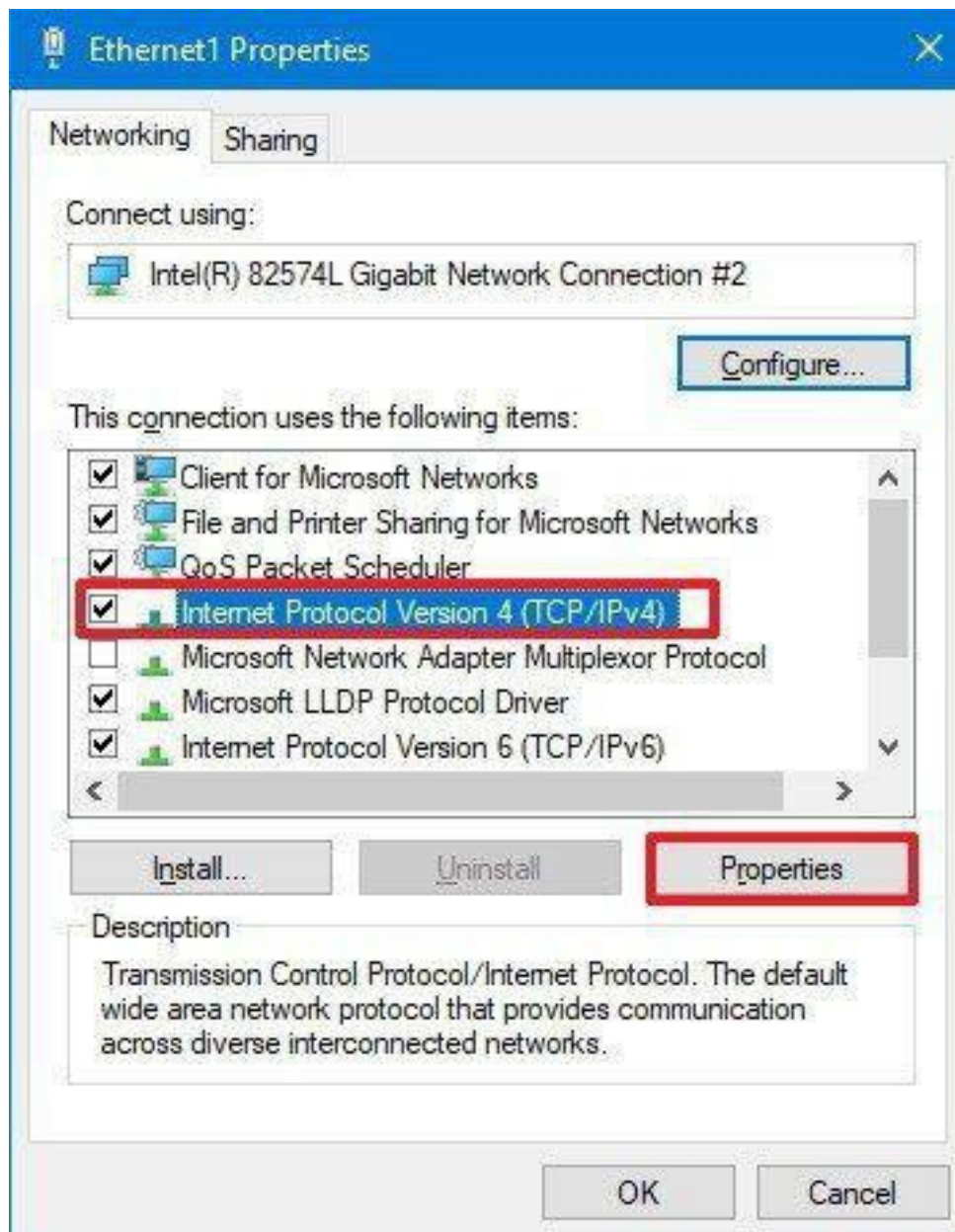
১. প্রথমে Start মেনুতে যান।

২. Control Panel এ যান।

৩. Network and Internet এ ক্লিক করুন।

৪. Network and Sharing Center এ ক্লিক করুন।

৫. Change Adapter Settings

৬. Wi-Fi কিংবা Ethernet adapter যেটা ব্যবহার করে আপনি ইন্টারনেট এ সংযুক্ত আছেন সেটাতে রাইট-ক্লিক করুন এবং Properties সিলেক্ট করুন।

৭. Internet Protocol Version 4 (TCP/IPv4) অপশন সিলেক্ট করুন।

৮. Properties বাটনে ক্লিক করুন।

৯. Use the following DNS server addresses অপশন সিলেক্ট করুন।

১০. “Preferred DNS server” ফিল্ডে নিচের Ipv4 address দিন:

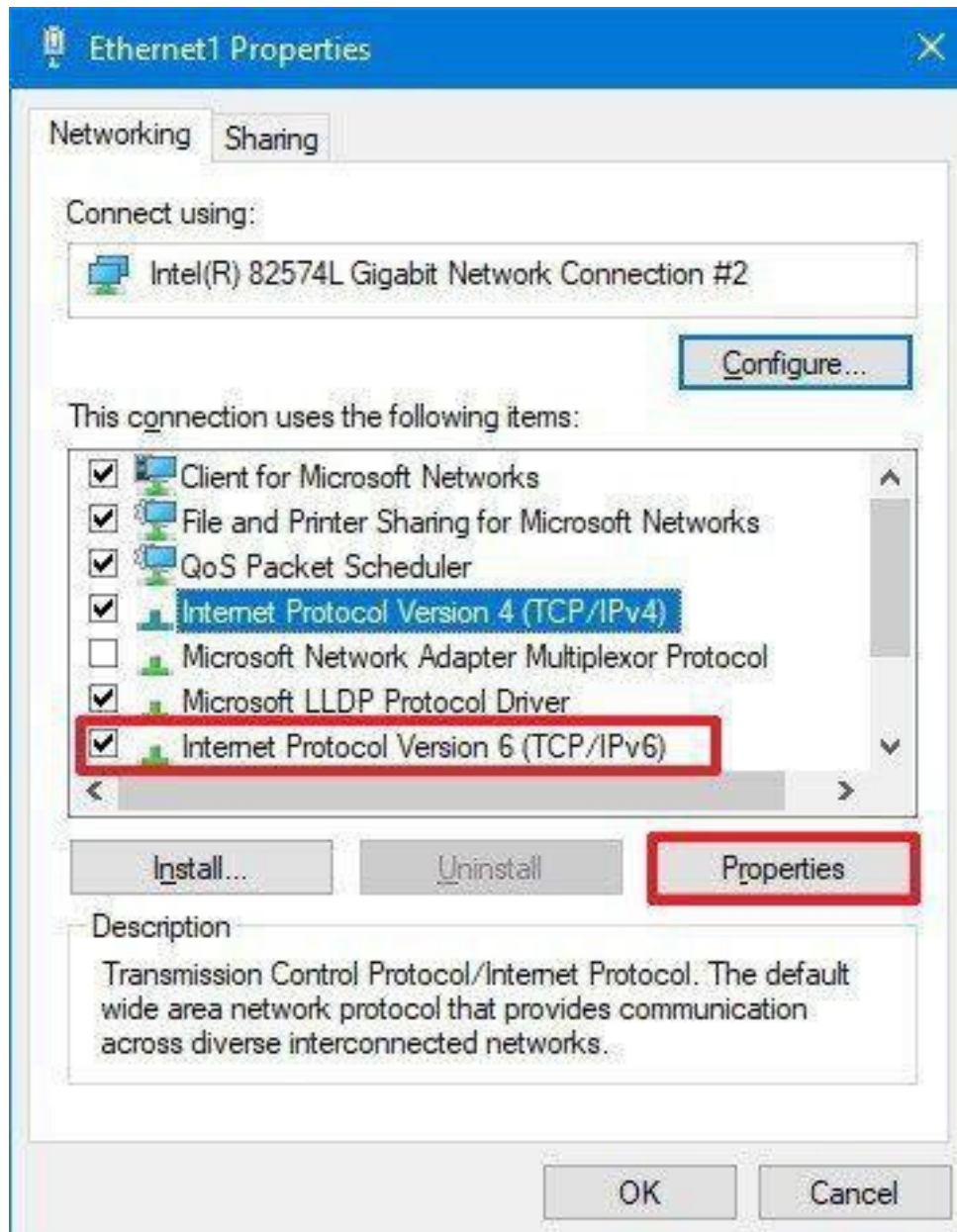
1.1.1.1

১১. “Alternative DNS server” ফিল্ডে নিচের Ipv4 address দিন:

1.0.0.1

১২. OK বাটনে ক্লিক করুন ।

১৩. (ঐচ্ছিক) যদি network adapter properties এ Internet Protocol Version 6 (TCP/IPv6) stack টি Enable করা থাকে তবে সেটি select করুন ।

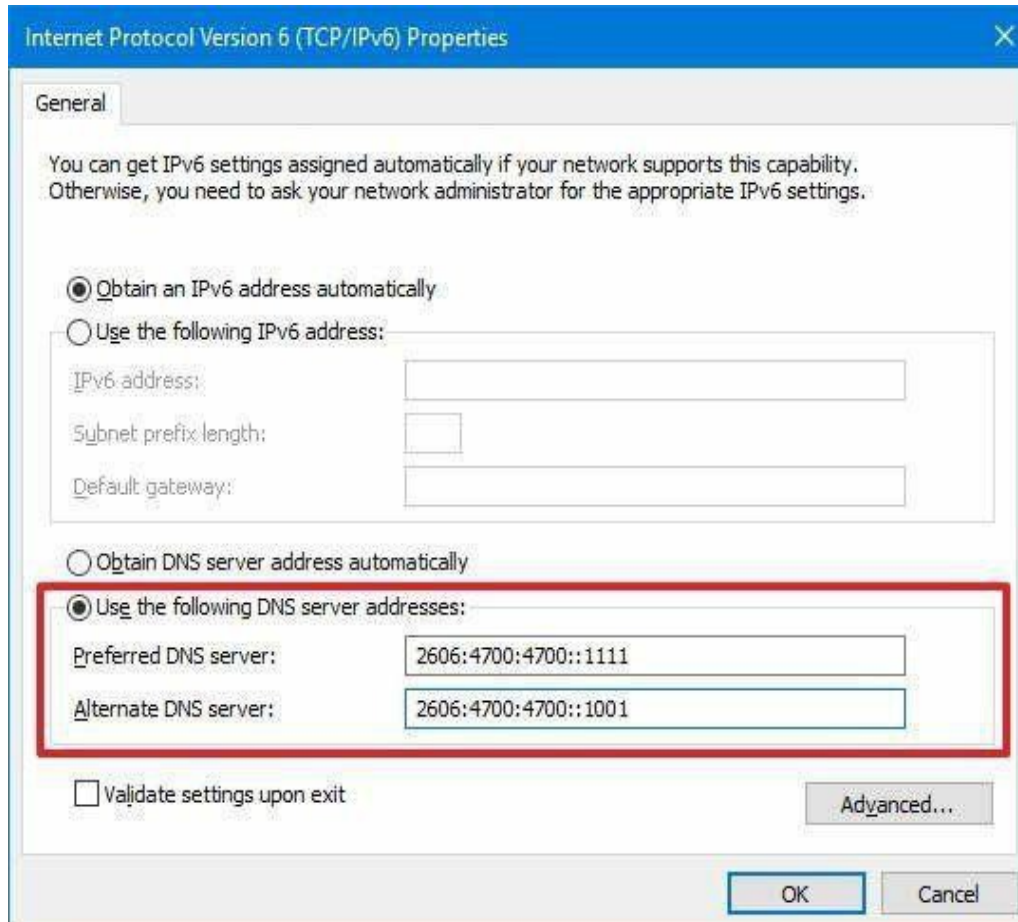
১৪. Properties বাটনে ক্লিক করুন।

১৫. Use the following DNS server addresses অপশন সিলেক্ট করুন ।

১৬. "Preferred DNS server" ফিল্ডে নিচের IPv6 address টি দিন :

2606:4700:4700::1111

১৭. "Alternative DNS server" ফিল্ডে নিচের IPv6 address দিন :

2606:4700:4700::1001

১৮. OK ক্লিক করুন ।

১৯. Close বাটনে ক্লিক করুন ।

এই স্টেপগুলো সমাপ্ত করার পর আপনার ডিভাইস বিভিন্ন ডোমেইন নেম (যেমন - Google.com অথবা WindowsCentral.com) খোঁজার জন্য Cloudflare সার্ভারে যোগাযোগ করবে।

উপরে বর্ণিত স্টেপগুলো Windows 10 অনুসারে দেখানো হয়েছে। কিন্তু এগুলো Windows 8.1 এবং Windows 7 এও কাজ করবে।

IP adress কি???

ইন্টারনেট প্রটোকল এড্রেস তথা আইপি এড্রেস হল নেটওয়ার্ক সংক্রান্ত হার্ডওয়ার সনাক্ত করার জন্য ব্যবহৃত একটি নাম্বার।

আইপি এড্রেসের সাহায্যেই একটি ডিভাইস অন্য আরেকটি ডিভাইসের সাথে ইন্টারনেটের মত আইপি ভিত্তিক নেটওয়ার্কে যোগাযোগ করতে পারে।

বেশির ভাগ আইপি এড্রেস দেখতে এমনঃ

151.101.65.121

অন্যান্য ক্ষেত্রে আমরা এমন আইপি এড্রেস ও দেখে থাকিঃ

2001:4860:4860::8844

IP Address এর দুটি version রয়েছেঃ Ipv4 এবং Ipv6 . প্রথমটি (Ipv4) পুরাতন এবং বর্তমানে এটি আউটডেটেড হয়ে গেছে যেখানে Ipv6 হল আপগ্রেডেড IP version.

বিভিন্ন ধরনের আইপি এড্রেসঃ

Private IP Addresses

Public IP Addresses

Static IP Addresses

Dynamic IP Addresses

আইপি এড্রেস কি কাজে ব্যবহৃত হয়?

যদি আমি বিদেশি কোনো বন্ধুকে কিছু পাঠাতে চাই, তবে আমাকে তার সুনির্দিষ্ট ঠিকানা জানতে হবে। এটা যথেষ্ট নয় যে আমি শুধু তার নাম ব্যবহার করে পার্সেল পাঠিয়ে দিব আর আশা করব যে এটা তার কাছে পৌছে যাবে। বরং আমাকে সেখানে যথাযথ ঠিকানা লিখে দিতে হবে যা আমি এড্রেস বুক থেকে পেতে পারি।

ইন্টারনেটে ডেটা সেন্ডিং এর ক্ষেত্রেও একই পদ্ধতি ব্যবহৃত হয়। যদিও এক্ষেত্রে ফোনবুকে কারো নাম ব্যবহার করে তার ঠিকানা বের করার পরিবর্তে আপনার কম্পিউটার কোনো একটি Hostname এর IP Adress খোঁজে পাওয়ার জন্য DNS server ব্যবহার করে।
উদাহরণস্বরূপ, যখন আমি ব্রাউজারে www.google.com এর মত কোনো ওয়েবসাইটে প্রবেশ করি তখন সেই পেজটি লোড করার জন্য আমার রিকুয়েস্টটি DNS server এ পাঠানো হয়। DNS server তখন এই হোস্টনেম (www.google.com) এর জন্য নির্ধারিত IP Address (2001:4860:4860::8888) খোঁজে বের করে। IP Address খোঁজে না পেলে আমার কম্পিউটার বুঝতেই পারবে না আমি কি চাচ্ছি।

এখন, IP Address কিভাবে পরিবর্তন করব???

ভাল প্রশ্ন। অনেকভাবে আইপি এড্রেস পরিবর্তন করা যায়। তবে সর্বোৎকৃষ্ট হল VPN (Virtual Private Network) ব্যবহার করা। তাছাড়া আপনি proxy, Socks5, Tor, Turbo ইত্যাদি ব্যবহার করেও আইপি এড্রেস পরিবর্তন করতে পারেন। তবে যেহেতু এটা আপনার ব্যক্তিগত নিরাপত্তার বিষয় তাই আমি এক্ষেত্রে Express VPN এর মত Paid VPN ব্যবহারের পরামর্শ দেব। যতটুকু জানি এখনও পর্যন্ত তাদের বিরুদ্ধে কোনো রিপোর্ট নেই যেখানে অন্যান্য ভিপিএন প্রোভাইডাররা ক্লাইন্টের তথ্য সরকারি এজেন্ট কিংবা অন্যদের কাছে টাকার বিনিময়ে বিক্রি করে।
পেইড ভিপিএন ব্যবহারের জন্য আপনাকে খুব বেশি টাকা ব্যয় করতে হবে না অথচ আপনার এই সামান্য সতর্কতা কারাগারে বছরের পর বছর আটকে থাকা থেকে রক্ষা করতে পারে বিইযনিল্লাহ। কাজেই পেইড ভিপিএন ব্যবহার করুন, ফ্রি ভিপিএন ব্যবহার করা থেকে বিরত থাকুন।

অনেক মানুষ আছে যারা টর ব্যবহার করে এই ভেবে যে এটা ফ্রি এবং এর সার্ভিস পুরো বুলেটপ্রুফ। কিন্তু আপনি হয়ত জানেন না টর তৈরি করেছে মার্কিন সরকার । ভেবে দেখুন, ফেসবুকে একাউন্ট খুলা একদম ফ্রি। তাই মানুষ ফেসবুকে তাদের প্রকৃর তথ্য দিয়ে একাউন্ট খোলে, এভাবে ফেসবুকের কাছে সেই ব্যক্তির তথ্য চলে যায়, তার নাম, ঠিকানা, ফোন নাম্বার, কর্মস্থল সবকিছু। সাধারণ মানুষকে প্ররোচিত করা খুবই সহজ। কাজেই যেহেতু TOR একদম ফ্রি এবং খুবই স্লো, তাই সকল ক্লায়েন্ট যারা টর ব্যবহার করে তারা সবাই মার্কিন সরকারের কাছে অরক্ষিত (Unprotected/Vulnerable).

আপনি Cyberghost VPN ব্যবহার করতে পারেন।

কিংবা আপনি HMA (Hide My Ass) ব্যবহার করতে পারেন।

আচ্ছা, আমরা এটা এখানেই শেষ করতে চাই কেননা আমাদের আরো অনেক বিষয়ে আলোকপাত করতে হবে।

তো এখন আপনার Mac address, DNS address এবং IP address পরিবর্তিত হয়েছে। আলহামদুলিল্লাহ।
এখন আপনি মোটামুটি এনোনিমাস (ইন্টারনেটে নিজের পরিচয় কিংবা লোকেশন গোপন রাখা) দাবি করতে পারেন নিজেকে। কিন্তু এরপরও বিভিন্নভাবে আপনার পরিচয় প্রকাশিত হয়ে যেতে পারে। আমি এখানে প্রধান তিনটি উপায় নিয়ে আলোচনা করব যেগুলোর মাধ্যমে আপনার পরিচয় প্রকাশিত হয়ে যেতে পারে।

#Phishing

#Keylogger

#Social Engineering

Phishing কি???

Phishing হল একধরণের সাইবার ক্রাইম যেখানে কোনো ব্যক্তি এক বা একাধিক টার্গেটকে ইমেল, টেলিফোন কিংবা টেক্সট মেসেজের মাধ্যমে নির্ভরযোগ্য প্রতিষ্ঠানের রূপ ধরে নানা ধরণের প্রলোভন দেখিয়ে বিভিন্ন স্পর্শকাতর তথ্য যেমন ব্যক্তিগত পরিচয়, ব্যাংকিং এবং ক্রেডিট কার্ডের তথ্য কিংবা পাসওয়ার্ড হাতিয়ে নেয়ার প্রয়াস চালায়। এই তথ্য পরবর্তীতে গুরুত্বপূর্ণ একাউন্ট সমূহে প্রবেশ করতে ব্যবহার করে এবং এতে পরিচয় হাতিয়ে নেয়া কিংবা আর্থিক ক্ষতির স্বীকার হতে হয়।

এখানে KmowBe4 এ প্রকাশিত একটি ইমেজ দেয়া হল যেখানে ফিশিং ইমেল এ সাধারণভাবে লক্ষণীয় ২২ টি সোশ্যাল ইঞ্জিনিয়ারিং রেড ফ্ল্যাগ তুলে ধরা হয়েছে।

Phishing থেকে বাঁচার উপায়-

=> যে কোনো লিংকে ক্লিক করার আগে চেক করে নিন সেটা আসল না নকল।

=> যদি সন্দেহজনক কোনো লিংক চোখে পড়ে তাহলে সেটি কপি করে ভাইরাস টোটাল এ পেস্ট করে চেক করে নিন। https://www.virustotal.com/#/home/url
এখানে আপনি যেকোনো সন্দেহজনক ফাইল ও চেক করতে পারবেন।
=> কখনো **.exe** দিয়ে শেষ হওয়া কোনো লিংক এ ক্লিক করবেন না। এই ধরণের প্রোগ্রাম আপনি ক্লিক করার সাথে সাথে অটোমেটিক ভাবে চালু হয়ে যাবে।
কাজেই সর্বদা (.exe) ব্যাপারে সতর্ক থাকুন।

Keylogger কী???

কী লগার, স্পাইওয়্যার কিংবা মনিটরিং সফটওয়্যার যাই বলা হোক না কেন, এটি আসলে ডিজিটাল নজরদারির মত একটি বিষয় যার মাধ্যমে আপনার প্রতিটি ক্লিক/টাচ, ডাউনলোড এবং কথোপকথন ট্র্যাক করা সম্ভব।

কী লগার (কীস্ট্রোক লগার এর সংক্ষিপ্ত রূপ) হল একটি সফটওয়্যার যেটি আপনার কীবোর্ডে টাইপকৃত সকল তথ্য ট্র্যাক কিংবা সংরক্ষণ করে, আর এ কাজটি সাধারণত গোপনে করে থাকে ফলে আপনি জানতেও পারবেন না যে আপনাকে মনিটর করা হচ্ছে। এটা মূলত আপনার একাউন্ট ইনফরমেশন, ক্রেডিট কার্ড নাম্বার, ইউজার নেম, পাসওয়ার্ড এবং অন্যান্য ব্যক্তিগত তথ্য চুরির মত অসৎ উদ্দেশ্যে করা হয়ে থাকে।

আপনি কিভাবে একটি কী লগার সনাক্ত করবেন?

কী লগার সনাক্ত করার জন্য আপনাকে একটু সতর্ক হতে হবে। কিছু লক্ষণ যেগুলো কী লগার থাকার সম্ভাবনা প্রকাশ করেঃ

ইন্টারনেট ব্রাউজিং এর সময় অনেক বেশি স্লো হয়ে যাওয়া, মাউস কিংবা কীস্ট্রোক (কীবোর্ডে টাইপিং) আটকে যাওয়া অথবা আপনি যেটা টাইপ করছেন সেটা স্ক্রীনে না দেখানো কিংবা গ্রাফিক বা ওয়েব পেজ লোডিং এর ক্ষেত্রে Error আসা।

নিজেকে কিভাবে সুরক্ষিত রাখবেন?

যেমনভাবে আপনি দৈনিক নিয়ন্ত্রিত খাবার খেয়ে, পর্যাপ্ত বিশ্রাম এবং ব্যায়ামের মাধ্যমে আপনার স্বাস্থ্কে সুরক্ষিত রাখেন, ঠিক সেভাবে আপনার কম্পিউটার কিংবা মোবাইল ডিভাইসেরও স্বাস্থ্যকে সুরক্ষিত রাখতে হবে।
অর্থাৎ, এমন কিছু করা থেকে বিরত থাকা যা আপনার কম্পিউটার, স্মার্টফোন কিংবা ট্যাবলেট এর উপর বিরূপ প্রভাব ফেলতে পারে, যেমন – বিপজ্জনক ওয়েবসাইট ভিজিট কিংবা ভাইরাসে আক্রান্ত প্রোগ্রাম, ভিডিও অথবা গেম ডাউনলোড করা। এখানে কিছু টিপস দেওয়া হলঃ

=>যেকোনো এটাচমেন্ট সতর্কতার সাথে ওপেন করুন – ইমেল, P2P নেটওয়ার্ক, চ্যাট, সোশ্যাল নেটওয়ার্ক এ প্রাপ্ত এটাচমেন্ট ফাইল (ইমেজ, ভিডিও, অডিও কিংবা সফটওয়্যার) এমনকি মোবাইলের সাধারণ টেক্সট মেসেজেও কী লগার যুক্ত ম্যালিশিয়াস সফটওয়্যার এমবেড করা থাকতে পারে।

=>পাসওয়ার্ড ব্যবহারে সতর্কতা – চিন্তাভাবনা করে One-time পাসওয়ার্ড ব্যবহার করুন। গুরুত্বপূর্ণ যেসব সাইটে লগ ইন করেন সেগুলো Two-step verification ব্যবহার করে কি না যাচাই করে নিন।

=> ভিন্ন কোনো কিবোর্ড লেআউট ব্যবহার করতে পারেন – প্রায় সকল কী লগার সফটওয়্যারই QWERTY লেআউট এর উপর ভিত্তি করে নির্মিত। কাজেই আপনি যদি ভিন্ন লেআউট যেমন DVORAK ব্যবহার করেন তাহলে কী লগার কর্তৃক চুরি করা কীস্ট্রোক সমূহ অর্থবোধক হবে না যদি না কনভার্ট করা হয়।

=> একটি Comprehensive Security Solution ব্যবহার করুন – আপনার পিসি, ম্যাক, স্মার্টফোন-ট্যাবলেট তথা সকল ডিভাইস McAfee LiveSafe এর মত Security Solution এর মাধ্যমে সুরক্ষিত রাখুন যা একইসাথে Antivirus, Firewall এবং Identity & Data Protection এর সুবিধা প্রদান করে।

সোশাল ইঞ্জিনিয়ারিং (Social Engineering) কী??

Social Engineering হ্যাকারদের কাছে অত্যন্ত শক্তিশালী একটি টুল; এটা এতটাই শক্তিশালী যে FBI, CIA সহ সকল গোয়েন্দা সংস্থা তাদের ভিকটিম এর তথ্য সংগ্রহের জন্য এটি ব্যবহার করে থাকে। মূলত এটা হল বিভিন্ন ধরনের ট্রিক ব্যবহার করা যতক্ষণ না আপনি সফল হচ্ছেন।

বোঝার সুবিধার্থে আমি কিছু উদাহরণ দিচ্ছি –

ধরে নিন আপনি আমার টার্গেট। আমি আপনাকে ধরার জন্য আপনার আইপি এড্রেস এবং আপনার হোম এড্রেস পেতে চাই। এক্ষেত্রে আমি কিভাবে অগ্রসর হব?? আমি বিভিন্ন ধরনের টুল, সফটওয়্যার, এপ্লিক্যাশন ব্যবহার করতে পারি। যেমন- আমি Wireshark ব্যবহার করতে পারি। এই Application টি কিভাবে কাজ করে?
আমি এই এপ্লিক্যাশন টি ওপেন করে আমার ওয়েব ব্রাউজারে আপনার সাথে চ্যাট করব। আমি আপনাকে জিজ্ঞাসা করব আপনি কেমন আছেন কিংবা এরকম সাধারণ কিছু কথা বলব এবং আপনি আমার কথার জবাব দিবেন। কিন্তু আপনি জানেন না আমার পিসিতে সকল ইনকামিং এবং আউটগোয়িং আইপি এড্রেস রেকর্ড করার সফটওয়্যার চালু রয়েছে। কাজেই যখন আমি আপনার আইপি এড্রেস পেয়ে যাবো তখন আমি স্বাভাবিক ভাবে আপনাকে ধন্যবাদ, আপনি খুব ভাল মানুষ, আপনার সাথে সাক্ষাৎ হয়ে ভাল লাগল ইত্যাদি বলে আপনার থেকে বিদায় নিব এবং আপনিও খুবই খুশি হবেন। কিন্তু আপনি জানেন না ইতিমধ্যে আপনাকে হ্যাক করা হয়ে গেছে, কেননা আপনার আইপি এড্রেস পেয়ে যাওয়া মানে আমি আপনার নির্ভুল ঠিকানা খোজে বের করতে পারব।
এক্ষেত্রে আপনি যদি ভিপিএন কিংবা আইপি চেঞ্জার ব্যবহার করেন তবে আমি আপনার ফেইক আইপি এড্রেস পাব, তাহলে আমি কিভাবে আপনাকে হ্যাক করব? আমাকে অন্য উপায় অবলম্বন করতে হবে। যেমন ধরুন আমি একটি নতুন একাউন্ট খুললাম। হতে পারে এটা ফেসবুক, টেলিগ্রাম, হুয়াটসএপ ইত্যাদি। আমি আমার একাউন্ট টা এমনভাবে তৈরি করব যেন আমাকে খুবই নীরিহ, অত্যন্ত ভাল মানুষ মনে হয়। অতঃপর আমি আপনার সাথে খুবই সাধারণ ভাব নিয়ে চ্যাট করা শুরু করলাম। "দেখুন এরা কি করছে, এটা করা কি ঠিক হচ্ছে??" আপনি আমার সাথে একমত হলেন। একদিন আমি আপনার বিশ্বাস অর্জনের জন্য আপনার মাধ্যমে কোনো সেবামূলক কাজের দানের জন্য টাকা অফার করলাম কিংবা এরকম আরো কিছু করলাম বা বললাম। এবং কয়েক সপ্তাহ কিংবা মাস পর আপনি আমাকে

বিশ্বাস করবেন।

তখন আমি আপনাকে জিজ্ঞাসা করব আপনি কোথায় থাকেন, আপনার অবস্থা কেমন, আপনার পরিবারের সবাই ঠিক আছে কি না। আমি এক এক করে তথ্য সংগ্রহ করছি। আমি আপনাকে কয়টা বাজে জিজ্ঞাসা করতে পারি, আপনি হয়ত ভাববেন সময় বললে কি আর হবে। কিন্তু আপনার ধারণা ভুল। আপনি যখন এই ক্ষুদ্র তথ্য আমাকে দিবেন আমি তখন আপনি কোন মহাদেশে আছেন তা সনাক্ত করে ফেলব। অতঃপর যখন ঐ মহাদেশে কোনো বিশেষ ঘটনা কিংবা কোনো ব্রেকিং নিউজ টাইপের কিছু ঘটবে তখন আমি আপনার সাথে সেই বিষয়ে কথা বলব, হতে পারে আপনি তখন বলবেন, “ওহ! এটা তো আমার প্রতিবেশি দেশ” কিংবা “আমি মর্মাহত, কেননা এটা আমার দেশ।”

আপনি হয়ত বুঝতে পেরেছেন আমি কোন দিকে অগ্রসর হচ্ছি।

তো এটাই হল সোশাল ইঞ্জিনিয়ারিং।

এই ট্রিক ব্যবহার করে CIA এর মত গোয়েন্দা সংস্থা অনেক হ্যাকারকে গ্রেপ্তার করেছে। তারা কোনো হ্যাকারকে ধরার জন্য আন্ডারগ্রাউন্ডে এসে হ্যাকার সেজে হ্যাকারদের সাথে সৈন্যদের বিরুদ্ধে কাজ করার জন্য আগ্রহ প্রকাশ করে এবং এভাবে অগ্রসর হতে থাকে। কয়েক মাস কিংবা বছর পর তারা পজিটিভ রেজাল্ট পায়।

আমি যেটা বলতে চাচ্ছি যে এই ফিল্ডটা অনেক বড়। এখানে আমি সব বিবরণ দিতে পারছি না, তবে আশা করি আপনি ইতিমধ্যে সোশাল ইঞ্জিনিয়ারিং সম্পর্কে মোটামুটি ধারণা পেয়ে গেছেন।

কাজেই যখন আপনি অনলাইনে থাকেন কখনোই আপনার ব্যক্তিগত তথ্য শেয়ার করবেন না এমনকি আপনার বেড়ালের কিংবা গাড়ির রঙ এর মত ছোটখাটো বিষয় ও না।

অনলাইনে যাওয়ার পূর্বে ও অনলাইনে কাজ শেষ করে Ccleaner অথবা BleachBit এর মাধ্যমে সকল Internet History, Cache, Cookies, Temporary files ডিলিট করে ফেলুন।

⚠⚠⚠ ভুলেও কোনো সন্দেহজনক লিংক এ ক্লিক করবেন না। যখন আপনি দেখবেন কেউ মেসেঞ্জারে কিংবা অন্য কোনোভাবে আপনাকে একটা লিংক পাঠিয়েছে , তখন আপনাকে প্রথমে যে কাজটি করতে হবে তা হল, লিংকটি কপি করবেন এবং এই সাইটের সার্চ বক্সে পেস্ট করবেন – https://www.virustotal.com/#/home/url

এই ওয়েবসাইটে গেলে আপনি একটি সার্চ বক্স পাবেন যেখানে লিংক পেস্ট করে ভাইরাস কিংবা ম্যালিশিয়াস এক্সিকিউটেবল ফাইল আছে কি না তা চেক করতে পারবেন। যদি আপনি Link/url চেক করতে চান তাহলে URL এ ক্লিক করবেন; আর যদি আপনি কোনো ফাইল ডাউনলোড করে থাকেন এবং সেটি চেক করতে চান তবে File এ ক্লিক করবেন। কিংবা আপনার পিসিতে কোনো ফাইল আছে, সেটি ওপেন করার পূর্বেও এখানে চেক করে নিতে পারেন সেটাতে ভাইরাস আছে কি না।

আমি আবারো বলছি কেননা আমরা প্রতিনিয়ত এই বিষয়টা এড়িয়ে যাই। আমরা সোশাল মিডিয়াতে বিভিন্ন জিনিস দেখি এবং কোনো চিন্তা ভাবনা ছাড়াই ক্লিক করে বসি। আমরা ভাবি এতে কিছুই হবে না।
তাহলে শুনুন, আমি আরেকটি ট্রিকি ভাইরাসের ব্যাপারে বলছি। সোশাল মিডিয়ায় আপনি অনেক পিকচার দেখলেন। একটি আপনার ভাল লাগল আর আপনি অধিক রেজুলুশান এর জন্য সেটাতে ক্লিক করলেন। আপনি যেটা ধারণাও করেন না তা হল একটি পিকচারের সাথে একটি ভাইরাস সংযুক্ত করে দেয়া সম্ভব এবং এটা অটোমেটিক্যালি এক্সিকিউটেবল আর আপনার এন্টিভাইরাসও এটা সনাক্ত করতে পারবে না। কাজেই যখন আপনি শুধু একটি পিকচারে ক্লিক করলেন প্রকৃতপক্ষে আপনি তখন ঐ ভাইরাসটিকে সেই ইমেজের পিছনে আপনার পিসিতে রান করার অনুমতি দিয়ে দিচ্ছেন। তাই ইন্টারনেটে এলোমেলোভাবে ক্লিক করা থেকে বিরত থাকুন।

যে টুলগুলো ব্যবহার করা অত্যাবশ্যকঃ

১. Ccleaner

২. Bleachbit

৩. Windows defender

8.Trend Micro Housecall

আপনি যদি Pro Anti-virus কিনতে সক্ষম হন তবে আমি পরামর্শ দেব –

 # ESET SMART SECURITY PREMIUM

অথবা

 # Bit Defender

⚠️ **আপনি কতটা নিরাপদ তা চেক করতে নিচের ওয়েবসাইট দুটিতে যান** ⚠️

১. https://www.ip-score.com

২. https://whoer.net

⚠️ ***এখানে আপনার আইপি লোকেশন যেটা দেখাবে অন্যেরাও ঠিক তাই দেখবে*** ⚠️

অনলাইনে নিরাপদে ব্রাউজিংএর জন্য কিছু বিশেষ টিপস –

কোন ব্রাউজার ব্যবহার করা উচিৎ?

- Chrome
- Firefox
- Safari
- Internet Explorer

আমার উত্তর হল এগুলোর একটিও ব্যবহার করবেন না।

 # Sphere ব্রাউজার ব্যবহার করুন।

যদি আপনি Sphere ব্রাউজার সম্পর্কে না জানেন তবে ইউটিউবে সার্চ করে জেনে নিন।

কোন সার্চ ইঞ্জিন ব্যবহার করা উচিৎ?

- Google
- Yahoo
- Bing

আমি বলব ***#DuckDuckGo*** ব্যবহার করুন।

DuckDuckGo সার্চ ইঞ্জিন অন্যদের মত আপনাকে ট্র্যাক করে না।

কোন VPN ব্যবহার করব?

1. Express VPN
2. Nord VPN
3. HMA

যদি আপনি প্রিমিয়াম ভিপিএন কিনতে সক্ষম হন তবে অবশ্যই প্রিমিয়াম ভিপিএন ব্যবহার করুন। এটা সর্বোত্তম। ভিপিএন এর ক্ষেত্রে আমার র‍্যাংকিং অনুসরণ করুন। সবচেয়ে ভাল Express VPN তারপর Nord VPN এবং সবশেষে HMA.
কিন্তু যদি আপনার মনে হয় যে আপনি প্রিমিয়াম ভিপিএন কিনতে সক্ষম নন, তারপরও আপসেট হবেন না। আপনার জন্যও ভাল এবং ফ্রি অপশন আছে।
Mozilla Firefox এ Anonymox add-ons ডাউনলোড করে নিতে পারেন কিংবা DOTVPN ব্যবহার করতে পারেন। এটা ভাল হবে ইনশাআল্লাহ।

প্রতিনিয়ত Zero-Day Attack আকারে নতুন নতুন Vulnerability আমরা দেখতে পাই। কাজেই সর্বশেষ আমি বলতে পারি এই ইনফরমেশন গুলো আপনাকে আপনার অনলাইন আইডেন্টিটি সুরক্ষিত

রাখতে সর্বোচ্চ সাহায্য করবে; কিন্তু আমি আপনাকে ১০০% গ্যারান্টি দিতে পারব না এবং এটা কেও পারবে না। যদি কেও দাবি করে যে সে আপনাকে অনলাইনে পরিপূর্ণ নিরাপত্তার ব্যবস্থা করে দেবে তাহলে আমি বলব সে একজন মিথ্যুক। কারণ সিকিউরিটি হল একটি ইল্যুশন।

সবশেষে আমি আপনাকে অনুরোধ করব নিজেকে লেইমার বানাবেন না। লেইমার কে?
ভাল প্রশ্ন। লেইমার হল সে যে শুধু নিজের কথাই চিন্তা করে, অন্যদের ব্যাপারে ভাবেনা। আমার এই প্রচেষ্টা কোনো নির্দিষ্ট ব্যক্তিকে উদ্দেশ্য করে নয়। আমি যা-ই করেছি মুহাম্মাদ (সাল্লাল্লাহু আলাইহি ওয়া সাল্লাম) এঁর উম্মাহর জন্য। আল্লাহ আজ্জা-ওয়া-জ্বাল তাঁকে জান্নাতুল ফিরদাউসের সর্বোচ্চ মাকাম দান করুন। আমিন।

যেহেতু আমি আমার সামান্য জ্ঞান এখানে শেয়ার করেছি এখন এটা আপনার দায়িত্ব যে আপনি অন্য ভাই-বোনদের সাথেও এটা শেয়ার করবেন।
আমাদের অনেক ভাই-বোন আছেন যারা অনলাইনে আল্লাহর জন্য কাজ করে যাচ্ছেন। এখন যেহেতু বিভিন্ন দেশে আমাদের মুসলিম ভাই-বোনেরা আছেন কাজেই প্রায়ই নিরাপত্তাজনিত কারণে তারা স্বাধীনভাবে কাজ করতে পারেন না। আমরা জানি, যদি আপনি সোশাল মিডিয়ায় স্বাধীনভাবে কাজ করেন তাহলে আপনাকে এরেস্ট করে কারাগারে ঢুকিয়ে দেয়া হবে।
তাই আমাদের জন্য অত্যন্ত গুরুত্বপূর্ণ হল যথাসম্ভব তাদেরকে কুফফার সরকার কর্তৃক গ্রেফতার কিংবা কারারুদ্ধ হওয়া থেকে বাঁচতে সাহায্য করা।

এই বইটি বেশি করে শেয়ার করুন। কমপক্ষে ৭ জন ভাই কিংবা বোনের সাথে শেয়ার করুন। হতে পারে আমার আপনার এই ক্ষুদ্র প্রয়াস আমাদের ভাই-বোনকে তাগুত কর্তৃক হয়রানি থেকে রক্ষা করবে।
এটা কি অনেক ভাল হবে না !!!
এটা সাদাকাহ জারিয়া হবে ইনশাআল্লাহ।

এই ছিল আমার পক্ষ থেকে আপনাদের জন্য পরামর্শ।

আল্লাহ আমাদের কাজকে কবুল করে নিন।
জাযাকাল্লাহু খাইর

TG@313C7R0_544D

আপনাদের একনিষ্ঠ দু'আয় আমাদেরকে ভুলবেন না